FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
214709US2PCT	
U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR	
09/926369	
INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE
PCT/FR00/00900	07 APRIL 2000
PRIORITY DATE CLAIMED	
23 APRIL 1999	

TITLE OF INVENTION

PROCESS FOR WATERMARKING IMAGES

APPLICANT(S) FOR DO/EO/US

Severine BAUDRY, et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

Request for Consideration of Documents in International Search Report
Notice of Priority / PCT/IB/304 / PCT/IB/308
Drawings (5 sheets)

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/926369	PCT/FR00/00900	214709US2PCT

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	$1040.00
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	$890.00
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$740.00
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	$710.00
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$890.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	11 - 20 =	0	x $18.00	**$0.00**	
Independent claims	1 - 3 =	0	x $84.00	**$0.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$890.00**	
☐ Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$890.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				**$0.00**	
TOTAL NATIONAL FEE =				**$890.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				**$0.00**	
TOTAL FEES ENCLOSED =				**$890.00**	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of **$890.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **15-0030** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

22850

(703) 413-3000

Surinder Sachar
Registration No. 34,423

Surinder Sachar
SIGNATURE

Marvin J. Spivak
NAME

24,913
REGISTRATION NUMBER

Oct. 22 2001
DATE

214709US

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF :

SEVERINE BAUDRY ET AL : ATTN: APPLICATION DIVISION

SERIAL NO: NEW U.S. PCT APPLN :
(Based on PCT/FR00/00900)

FILED: HEREWITH :

FOR: PROCESS FOR WATERMARKING: IMAGES

PRELIMINARY AMENDMENT

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Prior to a first examination on the merits, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend the claims as follows:

1. (Amended) Process for watermarking images for processing and transmission of stationary or video images including embedding a message in the images before their transmission by modifying data characteristic of the images, comprising performing a co-watermarking by periodic embedding of a binary matrix P into the image so as to determine on reception co-ordinates of an origin of the initial image and allow registration of the images received relative to this origin so as to make it possible to read the embedded message.

2. (Amended) Process according to Claim 1, wherein the co-watermarking binary matrix is a pseudo-random matrix P of size mxm obtained by symmetry of a binary m-sequence.

3. (Amended) Process according to Claim 1, further comprising building an image I_p of a size of the watermarked image by periodic repetition of the pseudo-random matrix P, and modifying luminance values of pixels with co-ordinates of the image which are homologous to those of the image obtained by periodic repetition of the co-watermarking matrix by a marking amplitude depending for each pixel on the value of the homologous pixel in the image obtained by periodic repetition of the watermarking matrix.

4. (Amended) Process according to Claim 2, wherein, to determine at reception the co-ordinates of the origin of the initial image, further comprising chopping the image received into blocks, summing the blocks to form a matrix M of size mxm, cross-correlating the matrix M with the co-watermarking binary matrix P by successive shifts of the matrix M relative to the matrix P, and taking as co-ordinates of the origin the co-ordinates for which the cross-correlation product is a maximum.

5. (Amended) Process according to Claim 1, wherein, to perform a watermarking on video images, further comprising transforming the image into blocks of DCT coefficients, embedding a message into the image by modulating the DCT coefficients so as to perform an adaptive marking in order to achieve invisibility of the embedded message upon the restoration of the image, and rendering the message robust to degradations by the use of a redundancy.

6. (Amended) Process according to Claim 5, further comprising associating with each bit b_i of the message to be embedded two coefficients of a block of DCT coefficients

and modifying the values of the two coefficients selected as a function of the binary value of the bit of the message to be embedded.

7. (Amended) Process according to Claim 6, wherein, to perform the watermarking, further comprising comparing a difference of absolute values of the pairs of coefficients chosen from each block with a specified threshold value S so as to modify the absolute value of one of them as a function of the binary state of the bit of the message to be embedded when the result of the comparison is less than the specified threshold value S.

8. (Amended) Process according to Claim 5, wherein, to read the watermark of a video image, further comprising decoding the pairs of DCT coefficients corresponding to the bits of the embedded message by comparing an absolute value of the difference of the absolute values of the pairs of coefficients with the specified threshold value S, comparing with a zero value the difference of the absolute values of the pairs of coefficients so as to determine a binary state of the corresponding embedded bits when the result of the comparison is less than the value of the threshold S or declaring the binary state of the embedded bits as being undetermined if the result of the comparison is greater than the value of the threshold S.

9. (Amended) Process according to Claim 1, further comprising performing a watermarking on all points of the image.

10. (Amended) Process according to Claim 1, further comprising performing a postprocessing on the images received so as to estimate quality and reliability of the embedded message by using redundancy of the embedded message.

11. (Amended) Process according to Claim 10, further comprising repeating the watermarking message on each video image during a specified number of times by comparing for each bit of the watermarking message a number of times it is received

according to a first state and the number of times it is received according to a second state, and comparing totalized values thus obtained with a specified threshold value determined by the Bernouilli binomial probability law.

IN THE ABSTRACT OF THE DISCLOSURE

Please delete the original Abstract, page 28, in its entirety and insert therefor:

ABSTRACT OF THE DISCLOSURE

A process for watermarking images that includes embedding into the images before their transmission a message by modifying the data characteristic of the images. Further, a co-watermarking is performed by periodic embedding of a binary matrix into the image to determine on reception the co-ordinates of the origin of the initial image and allow the registration of the images received relative to this origin so as to make it possible to read the embedded message. Such a process may find particular application to the transmission of stationary or video images.

REMARKS

Favorable consideration of this application, as presently amended, is respectfully requested.

The present preliminary amendment is submitted to place the above-identified application in more proper format under United States practice and to clarify features recited in the claims.

By the present preliminary amendment, the claims have been amended to no longer recite any reference numerals or multiple dependencies. The claims have also been amended to broaden their scope by no longer reciting the phrase "consists" and to recite the broader

term "comprising". The claims have also been amended to address other minor amendments to broaden their scope.

The Abstract has also been amended by the present response to be in more proper format under United States practice.

The present application is believed to be in condition for a full and thorough examination on the merits. An early and favorable consideration of the present application is hereby respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

(703) 413-3000
Fax No.: (703)413-2220
GJM/SNS:kst

I:\atty\SNS\214709us-pr.wpd

Marked-Up Copy
Serial No:

Amendment Filed on:
10-22-01

IN THE CLAIMS

--1. (Amended) Process for watermarking images for [the] processing and transmission of stationary or video images [of the type consisting in] including embedding a message [(1)] in the images before their transmission[, a message] by modifying [the] data characteristic of the images, [characterized in that it consists in] comprising performing a co-watermarking [(2)] by periodic embedding of a binary matrix P into the image so as to determine on reception [the] co-ordinates of [the] an origin of the initial image and allow [the] registration of the images received relative to this origin so as to make it possible to read the embedded message.

2. (Amended) Process according to Claim 1, [characterized in that] wherein the co-watermarking binary matrix is a pseudo-random matrix P of size mxm obtained by symmetry of a binary m-sequence.

3. (Amended) Process according to [either of Claims 1 and 2] Claim 1, [characterized in that it consists in] further comprising building an image I_p of [the] a size of the watermarked image by periodic repetition of the pseudo-random matrix P, and [in] modifying [the] luminance values [I(i,j)] of pixels with co-ordinates [(i,j)] of the image which are homologous to those of the image obtained by periodic repetition of the co-watermarking matrix by a marking amplitude depending for each pixel on the value of the homologous pixel in the image obtained by periodic repetition of the watermarking matrix.

4. (Amended) Process according to Claim 2, [characterized in that] wherein, to determine at reception the co-ordinates of the origin of the initial image, [it consists in] further comprising chopping the image received into blocks, [in] summing the blocks to form a matrix M of size mxm, [in] cross-correlating the matrix M with the co-watermarking binary matrix P by successive shifts of the matrix M relative to the matrix P, and [in] taking as co-ordinates of the origin the co-ordinates for which the cross-correlation product is a maximum.

5. (Amended) Process according to [any one of Claims 1 to 4] Claim 1, [characterized in that] wherein, to perform a watermarking [(1)] on video images, [it consists in] further comprising transforming the image into blocks of DCT coefficients, [in] embedding a message into the image by modulating the DCT coefficients [(9,..22)] so as to perform an adaptive marking in order to achieve invisibility of the embedded message upon the restoration of the image, and [in] rendering the message robust to degradations by the use of a redundancy.

6. (Amended) Process according to Claim 5, [characterized in that it consists in] further comprising associating with each bit b_i of the message to be embedded two coefficients of a block of DCT coefficients and [in] modifying [(10,...17)] the values of the two coefficients selected as a function of the binary value of the bit of the message to be embedded.

7. (Amended) Process according to Claim 6, [characterized in that] wherein, to perform the watermarking, [it consists in] further comprising comparing [(10) the] a difference of [the] absolute values of the pairs of coefficients chosen from each block with a specified threshold value S so as to modify [(13,...17)] the absolute value of one of them as a

function of the binary state of the bit of the message to be embedded when the result of the comparison is less than the specified threshold value S.

8. (Amended) Process according to [any one of Claims 5 to 7] Claim 5, [characterized in that] wherein, to read the watermark of a video image, [it consists in] further comprising decoding the pairs of DCT coefficients corresponding to the bits of the embedded message by comparing [(18) the] an absolute value of the difference of the absolute values of the pairs of coefficients with the specified threshold value S, [in] comparing [(20)] with [the] a zero value the difference of the absolute values of the pairs of coefficients so as to determine [the] a binary state of the corresponding embedded bits when the result of the comparison is less than the value of the threshold S or [in] declaring [(19)] the binary state of the embedded bits as being undetermined if the result of the comparison is greater than the value of the threshold S.

9. (Amended) Process according to [any one of Claims 1 to 8] Claim 1, [characterized in that it consists in] further comprising performing a watermarking on all [the] points of the image.

10. (Amended) Process according to [any one of Claims 1 to 9] Claim 1, [characterized in that it consists in] further comprising performing a postprocessing [(3; 23,... ,28)] on the images received so as to estimate [the] quality and [the] reliability of the embedded message by using [the] a redundancy of the embedded message.

11. (Amended) Process according to Claim 10, [characterized in that it consists in] further comprising repeating the watermarking message on each video image during a specified number of times by comparing [(2, 3)] for each bit of the watermarking message [the] a number of times it is received according to a first state and the number of times it is received according to a second state, and [in] comparing [(26) the] totalized values thus

obtained with a specified threshold value determined by the Bernouilli binomial probability law.--

IN THE ABSTRACT OF THE DISCLOSURE

Abstract (New).

5/prts

Process for watermarking images

The present invention relates to an image watermarking process for the processing and transmission of stationary or video images.

In telecommunication, image watermarking is the act of transmitting information in an image or a sequence of images without entailing perceptible modifications in the composition of the image or of the image sequence received. This procedure is also sometimes known as "watermarking".

This definition recalls that of steganography, also called transmission by subliminal channel, which is the art of sending messages in a hidden manner, a seemingly innocent piece of information containing a hidden message which can be read only by the rightful recipients. Unlike cryptography, steganography conceals the very existence of the subliminal message.

The essential difference between image watermarking and steganography resides in the choice of what is called the "cover channel", namely the plaintext message which contains the hidden message.

In steganography, the sender can make this choice himself, whereas in the case of watermarking it is imposed. The motivations of the two techniques are also not the same since the sender of a steganographic message wishes to be able to communicate secret information without arousing the suspicions of a sentry, whereas the sender of a watermarked image wishes that the hidden message should not perceptively disturb a work and should not be easily scrambled, but the fact that anybody may possibly be informed of the presence of a hidden message in an image is not problematic, quite the contrary it may have a beneficial deterrent effect when for example the

watermark is intended to be used as a sign enabling the images to benefit from the protection afforded by royalties and copyright in particular. In this case the watermark is produced by embedding in an image or a sequence of images a piece of information which characterizes the work and its owner. Automatic read-out of the embedded information makes it possible to check whether the work has not been broadcast illegally, or else to check whether the author has indeed received the corresponding royalties. Image watermarking also makes it possible to track documents when the embedded information is characteristic of the person who has bought it, this making it possible, upon elicit copying or distribution, to automatically ascertain who is responsible for the fraud.

The same holds for all automatic image or image sequence indexing applications.

The attraction of using watermarking lies in the possibility of making the checks automatic. It is in fact utopian to contemplate manually checking the broadcasting of audio-visual works, given the multiplicity of transmission channels. The watermarking of images enables this problem to be partially solved by making it possible, starting from a work, to automatically determine its identifying number and possibly its source, it subsequently being up to the society of authors to determine whether the work has indeed been broadcast illegally. The techniques of watermarking also offer the advantage of not requiring any standardization or prior agreements between the various parties unlike the current practice with regard to hardware protection against copying incorporated into digital video discs also known by the abbreviation "DVD" standard for "Digital Video Disc".

To be able to transmit a message through an image, the latter has to be modified in one way or another. The

modifications made by watermarking must however satisfy a certain number of conditions so as to be able to be compatible with the applications envisaged.

Thus, the watermark should not visibly modify the images so as not to degrade their quality. Consequently, the marking must be discreet.

As will be shown later, many watermarking methods described in the literature require the presence of the original image in addition to the modified image when reading the message. Hence, these methods seem to be wholly unsuitable for the protection of works by copyright since they assume that the author has labelled a work apparently belonging to him and broadcast illicitly, before being able to prove by the reading of the watermark that the work is indeed his own. In this case it is much faster to compare the two works than to read a watermark. The reading of a watermark from the modified image alone must therefore be possible for automatic "monitoring" applications. Watermarking methods using both images when reading may however be used for the tracking applications alluded to above, the identity of the work then being certain, the watermark merely making it possible to advise as to the source of the copy concerned.

Watermarking becomes a trivial problem if one is sure that the watermarked image will not be modified in any manner. It is then sufficient to modify the low-order bits of the pixels, this being a completely invisible manipulation and making it possible to embed as many bits as there are pixels. However, this ideal case is never encountered in practice, since images, and in particular image sequences, are almost always compressed to obtain an acceptable bit rate during transmission or to save memory space during storage. This compression may be lossless as is the case with the "JPEG useless" standard, but it is usually

irreversible for reasons of efficacy in the transmissions of images according to the JPEG and MPEG standards. It is consequently vital for the watermark to be able to survive these transformations, this being all the more difficult since the compression takes place at low bit rate. Consequently the marking must be sufficiently strong, this being a constraint which conflicts with the above invisibility constraint.

Neither is it rare for a work, during its broadcasting in particular, to be modified so as to aid transmission. Postproduction often introduces for example a "cropping", that is to say a chopping of the sequences. Their format may also be modified, in particular when switching from the American television standard (720x480 images at 30 Hz) to the European format (720x576 images at 25 Hz). Resamplings for magnifying or reducing the images are also frequent.

Within the context of the watermarking of images these transformations pose two types of problems, on the one hand, they are not in general reversible, this obviously being true upon chopping, and also upon an image reduction since a great deal of information is lost in the high frequencies of the image, and on the other hand, the transformation existing between the original image and the transformed image is not generally known. It follows that the watermark must either be invariant under geometrical transformation, or be accompanied by additional information allowing synchronization. This transformation may take the form of a particular watermark making it possible to determine the transformation performed.

Digital image and film manipulation is especially easy provided that the user has even very rudimentary image processing software. Geometrical transformations are among the simplest manipulations, they consist in particular in performing image chopping, magnifications

or reductions, montages of several sequences, collages and more rarely rotations. Frequency modifications are relatively easy, as are colorimetry manipulations consisting in switching from colour to black and white or the reverse for films, transformation of histograms etc. The possibility should also be noted of switching from digital to analogue or vice versa for image photocopying and video cassette digitizing operations etc., which involve additional noise as well as geometric or colorimetric distortions.

The watermark must also be resistant to deliberate attacks from pirates aimed at destroying the mark so as to be able to broadcast a work without paying royalties. The attack processes may be of two types, either they consist of attempts to reverse the marking procedure, blindly or with the aid of partial or complete knowledge of the marking algorithm, or by scrambling the message by adding noise or by transformation by filtering for example. The first type of attack can be countered using processes similar to those employed in cryptography using secret keys. In the second type of attack, the pirating must make a compromise between the force of the scrambling and the degradation in quality which results. This circumstance may moreover be exploited in order to produce a good watermark by marking with a force which is just less than the threshold of visibility, the entire problem being to determine this threshold accurately.

Finally, the watermark must be of low complexity. Complexity is a crucial problem for a real system. Whereas writing can sometimes be carried out off-line, it must necessarily be possible to perform reading on-line for "monitoring" applications, and it is frequently this step which is the most expensive in terms of computation time.

Although the field of watermarking is relatively recent, a large number of approaches have already been proposed in the literature. They call upon various methods of watermarking which may be classified into methods of spatial or pixelwise watermarking, transform-based or frequency-based methods of watermarking and coding-based watermarking methods.

Other approaches have also been studied, for watermarks of the audio, text or computer-generated image type propose [sic] a particular algorithm. Others propose a more general formulation of the problem, in particular in terms of information theory. The articles which describe them attempt to more accurately quantize the passband available for the watermarked message. Other articles present methods of attack specific to a particular or more general watermarking technique. In parallel, techniques of formalizing these attacks are appearing, using game theory or the concepts of cryptography and of steganography for example, aimed at allowing the devising of more robust systems.

In the methods of spatial watermarking, the writing of the message is performed directly in the plane of the image, generally by modifying the luminance of the pixels.

In the transform-based methods of watermarking the writing of the message is performed on a transform of the image or of a sequence. The transforms used are generally of the Fourier, cosine transform or wavelet types.

Finally, in the coding-based watermarking methods the watermark is embedded by directly modifying certain elements obtained during encoding. This relates for example to the motion vectors in MPEG coding, the blockwise or "matching blocks" coding of a fractal compression, etc. DCT coding methods by cosine

transform, abbreviated as "Discrete Cosine Transform" may also be included in this category.

These large families may also be divided into two subfamilies which cover the blockwise coding methods and the image coding methods. In the blockwise coding methods, of the DCT type or the pixelwise coding methods for example, the coding unit is the block in which one or more bits are embedded. In the image coding methods, the watermark is made on the image in a global manner, for example by using a global Fourier transform of the image.

The spatial methods are among the oldest and are the simplest. The advantage of these methods is that they allow generally faster writing of the watermark requiring no expensive transformations as is the case for example for methods based on the Fourier transformation. They are however less robust to compression techniques based on the calculation of DCT transforms.

Among the spatial watermarking methods the algorithm dubbed "patchwork" by Messrs Bender, Gruhl, Morimoto, a description of which may be found in the article entitled "Techniques for Data Hiding" published in the SPIE Proceedings, Vol. 2420, p. 40, Feb. 95 relies on the observations that the eye is rather insensitive to small changes of luminance, especially when they are random and akin to low-power noise and that the averages of the luminances of two sets of N points chosen randomly are "on average" equal when the number N is large.

In this algorithm, writing takes place using a secret key, and n pairs of points A_i and B_i respectively of luminance a_i and b_i, which are chosen in a pseudo-random manner in the image. The luminance of the chosen points is modified according to the relations $a_i' = a_i + 1$ and

$b_i' = b_i - 1$. Since the points are chosen randomly, the difference $a_i - b_i$ will on average be zero for N sufficiently large. On the other hand, the difference $a'_i - b'_i$ will on average be almost equal to 2, thereby allowing decoding.

To retrieve the initial points, reading takes place with the aid of the secret key. Calculation of the quantity $S=\sum_{i=0}^{N-1}(ai-bi)$ makes it possible to decide that the image is watermarked when $S \approx 2N$.

This method makes it possible to embed just one bit into the image, but it can be generalized onto several bits by choosing several disjoint sets of points. It has the advantage of exhibiting good invisibility, and good resistance to transformations such as compression, the addition of noise, etc., all the more so the larger the number N. It also exhibits good resistance to the chopping of the image, due to the dissemination of the information, and good resistance to attacks provided that the key is not known.

On the other hand it has the drawbacks of weak resistance to geometrical transformations and of demanding a compromise between the number of bits to be embedded and the resistance of the message.

Another method using amplitude modulation of the chrominance which is described in the article by Messrs Kutter, Jordan, Bossen entitled: "Digital Signature of Colour Image Using Amplitude Modulation" and published by SPIE EI 97 consists in modifying the blue component of the chrominance signal to which the eye is rather insensitive and in acting as a function of the marking force on the modulation of the luminance signal while allowing for the fact that the retina is more sensitive to contrasts than to luminance proper, the acuity of the eye being lower at high luminance. A zigzag scan is

performed so as to disregard the size of the image. Reading is performed by linear prediction. According to this method the message can be written in a robust manner by embedding the same bit several times. Zigzag scanning makes it possible to disregard the size of the image, and also to disregard synchronization should the bottom or the left of the image be chopped. The method also exhibits good resistance to attacks. On the other hand the complexity of the calculations becomes very significant in the case where geometrical transformations have to be performed, since this method requires an exhaustive search in the parameter space.

Another spatial watermarking method described by the authors Jean François Delaigle and Benoit Macq in Talisman Project Report Jan. 97 entitled "Digital Watermarking" implements an algorithm allowing the embedding of one bit per image block of dimension nxn. A block is divided into two groups of pixels A and B. The values of the pixels of the two groups are modified in such a way that the difference of the averages of the luminances of the groups A and B is the bearer of the bit to be transmitted. These modifications are carried out without modifying the global average of the luminances of the block so as to retain good invisibility. The marking force depends on a parameter I. This method yields a resistance to coding according to the JPEG standard of 70% with an error rate of 5% for a marking luminance level I=5. The marking is invisible for marking levels which are not too high for I<8, but the visibility and the robustness depend for a specified marking level on the size of the block. However, the method has a major drawback, namely of exhibiting low resistance to geometrical transformations and to attacks of the line deletion or column deletion type.

Coding methods based on frequency transforms, such as the one described in patent application DE 19521969,

are doubly attractive. On the one hand they make it possible to anticipate the compression by writing the watermarking information into the components of the image having the least chance of being modified and they make it possible on the other hand to allow for the perception characteristics of the human eye so as to mark more strongly in the least perceptible components.

These two aspects are nevertheless antithetical since the compression techniques rely specifically on the characteristics of the eye.

According to a first approach published by Messrs Eckhard Koch and Jian Zhao in the article entitled "Embedding Robust Labels into Images for Copyright Protection", proc.Int. Congr. Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, Austria August 95, the writing of the watermarking message is performed by modifying the coefficients of the DCT discrete cosine transform by anticipating the quantization noise introduced by the image compressions performed according to the JPEG or MPEG processes so as to ensure the survival of the watermark during these compressions. This approach makes it possible to obtain good resistance to compression since the quantization noise is no longer random noise since it is anticipated during the marking. The resistance depends of course on the quantization factor Q used during marking. The higher the factor Q, the better the robustness, although at the cost of an increase in visibility. The method is attractive also in that the watermarking algorithm can be implemented directly in a JPEG or MPEG coder, thus making it possible to profit directly from the calculations of the DCT coefficients performed during compression. However, the performance of the method may degrade very rapidly when the blocks of DCT coefficients of the image do not coincide with the

blocks of the original image, this occurring for example when the image has been slightly shifted, in this case the quantization noise is then no longer predictable.

Another method described by Messrs Ingemar Cox, Joe Killian, Thomson Leighton, Talal Shamoon in the article published in IEEE Trans. on Image Processing, Vol. 6 No. 12, Dec. 97 entitled "Secure Spread Spectrum Watermarking for Multimedia" carries out a "spread band" approach consisting in embedding the watermarking message into all the frequency components of the image after having calculated the DCT coefficients, thereby rendering the energy of the message on each of the frequencies indiscernible but, on the other hand, making the signal-to-noise ratio high. Visibility criteria are moreover used to weight the force of the marking according to the frequency components. The advantages of this method are of exhibiting very good resistance to JPEG and MPEG type compressions and of offering very good resistance to geometrical transformations provided that these transformations are known. The method offers multi-watermarking possibilities. It is good at resisting attacks by collusion by averaging over documents bearing different watermarks, and at resisting scrambling attempts since in the absence of knowledge of the watermarking message, it is necessary to add sufficiently strong noise to all the frequencies, thereby degrading the visual quality of the image, in order to destroy the watermark. However, the method has a major drawback, namely that it is necessary to have the original image in order to retrieve the watermark, the latter being obtained by subtracting the transformed watermarked image from the transformed original image.

Another method described in an article by Messrs Joseph O'Ruanaidh, Thierry Pun entitled: "Rotation, Scale and Translation Invariant Digital Image Watermarking",

published in the proceedings of IEEE ICIP 97 Vol. 1, p. 536-539 Santa Barbara, consists in using a space which is invariant under rotation, translation and scaling, in order to disregard the geometrical transformations which may be carried out on the image. This is achieved by exploiting the properties of the Fourier-Mellin transform. The method has the advantage of exhibiting high resistance to geometrical transformations without requiring prior synchronization. However, the invariance properties of the Fourier-Mellin transform are no longer complied with when the circular translation is replaced by a "cropping". Moreover, the calculations which demand transformations in a log-polar plane are relatively complex.

Another method described in the article by Messrs Joseph O'Ruanaidh, W. Dowling, F. Boland entitled "Phase Watermarking of Digital Images" published by ICIP 96 uses a Fourier transform, writing the watermarking message with the aid of a phase modulation. The method has the advantage of offering resistance to the JPEG and MPEG compression processes. However, it has the drawback that the phase modifications appear in a more visible manner than the amplitude modulations.

Another method described in the article by Messrs Mitchell Swanson, Bin Zhu, Ahmed Tewfik, entitled "Multiresolution Scene-based Video Watermarking Using Perceptual Models", published in IEEE journal on selected areas in communications, Vol. 16, No. 4, May 98, is specifically intended for the watermarking of video sequences. It consists in working in a transformed space obtained by decomposition into temporal wavelets using a perceptual model. According to the method a watermarking message is generated with the aid of two keys, one corresponding to the information to be transmitted and the other calculated

with the aid of the original video sequence. The second key makes it possible to solve the known problem of the deadly embrace, that is to say to prevent a pirate from rewatermarking a sequence with his own message and subsequently claiming priority of his watermark. This information is encrypted with the aid of a BBS generator. The video sequence is subsequently segmented into scenes, and each scene is decomposed into temporal wavelets so that the statistical components of the scene are made to appear in the low frequencies and the dynamic elements of the scene are made to appear in the high frequencies. A spatial perceptual mask is calculated for each wavelet coefficient, then each wavelet coefficient is decomposed by calculation of DCT coefficients so as to set up a frequency mask and perform a shaping of the watermark with the aid of the masks thus determined and apply it to the temporal wavelets. To detect the watermarking message at reception it is necessary to ascertain the original sequence and also the embedded watermarking message. This can be achieved without any temporal synchronization information being required regarding the sequence recovered. The method has the advantages of exhibiting good resistance to the modifications performed on the video sequences, of being able to make fine allowance for visibility through the use of masking criteria and of exhibiting high redundancy in the writing of the information which takes place in several frequency bands. The drawback of this method resides however in the fact that it requires the use of the original sequence for the reading of the watermark and that it allows the embedding of a single bit only.

In coding methods the watermark is embedded by modifying certain elements obtained when coding an image such as for example the motion vectors of the coding according to the MPEG standard or the "matching blocks" of fractal compression. These methods make it possible to work directly in the encoded images, thus

allowing faster writing and above all faster reading of the watermark. They also allow better consideration of the distortions introduced by the coding. Unfortunately, this consideration may become ineffective when re-encoding with different parameters.

A first method of watermarking described by Messrs T. Vynne, F. Jordan, in an article entitled "Embedding a Digital Signature in a Video Sequence using Motion Vectors" pre-print of special session on copyright protection and access control for multimedia services of ICIP 96, consists in writing the watermarking message by modifying the motion vectors of the MPEG coding process. The coding procedure commences by choosing a set of blocks in the image to embed the watermarking information and by calculating for each of the blocks the optimal motion vector with respect to the previous image. The writing of the message is performed by modifying the low-order bit of the components of the motion vector. The visibility of the watermark can be reduced by making sure that the block variances obtained with the aid of the original motion vector and of the modified motion vector are much the same. The advantage of this method is that it allows direct watermarking in the MPEG transmission stream. On the other hand, the method is sensitive to the motion estimators used and to re-encoding.

A second coding method of the authors Joan Puate, F. Jordan, described in an article entitled: "Using Fractal Compression Scheme to Embed a Digital Signature into an Image", proc.SPIE Video Techniques and Software for Full-Service Networks, Oct. 96, consists in writing the watermark by modifying the parameters used in fractal coding. The robustness of the method depends on the size of the image partition blocks used to carry out the coding. The bigger the size of the blocks, the more robust the method, but the worse the quality of

the image obtained. Moreover, the computation time is considerable.

The aim of the invention is to alleviate the aforesaid drawbacks.

Accordingly, the subject of the invention is a process for watermarking images for the processing and transmission of stationary or video images of the type consisting in embedding in the images before their transmission, a message by modifying the data characteristic of the images, characterized in that it consists in performing a co-watermarking by periodic embedding of a binary matrix P into the image so as to determine on reception the co-ordinates of the origin of the initial image and allow the registration of the images received relative to this origin so as to make it possible to read the embedded message.

The process according to the invention has the advantage that it makes it possible to perform watermarking which is at the same time robust, reliable and of low complexity.

The invisibility of the watermark is complete, even on professional viewing equipment of very high quality.

Unlike the aforesaid prior art processes, the watermark can be read out without needing the unwatermarked original image, this making it possible to apply the process to the automatic checking of broadcasts.

The marking is good at resisting MPEG and JPEG compressions.

The co-watermarking process implemented also offers resistance to image chopping, this being important given the current video coding and transmission systems. The low complexity of this algorithm in terms of reading constitutes a definite advantage relative to

the methods of synchronization by exhaustive search such as the EPFL's spatial algorithm for example.

Finally, it also makes it possible to be sure of the reliability of the message read out, by giving information regarding the quality of this message. The error rate for the final message, as well as the decision latency time can be parametrized to accommodate the constraints of each application.

Other characteristics and advantages of the invention will become apparent with the aid of the description which follows in conjunction with the appended drawings which represent:

Figure 1 the main steps of the processing for carrying out the transmission of an image watermark according to the invention.

Figures 2 and 3 an illustration of the method of watermarking by coding by DCT transform implemented according to the invention.

Figure 4 a flowchart illustrating the procedure for mapping the DCT watermarking coefficients over the entire image, implemented by the invention.

Figures 5 and 6 the various steps of the watermarking procedure according to the invention, depicted as a flowchart.

Figure 7 the obtaining of a co-watermarking matrix according to the invention.

Figure 8 a diagram illustrating the principle of writing of a co-watermark according to the invention.

Figure 9 a diagram illustrating the principle of reading of a co-watermark according to the invention.

Figure 10 some steps of the postprocessing performed by the invention depicted in the form of a flowchart.

The watermarking process for the transmission of images according to the invention which is represented in Figure 1 implements three algorithms, a basic watermarking algorithm 1 which makes it possible to embed the watermarking message into the image, a co-watermarking algorithm 2 allowing spatial resynchronization of the image when the latter has undergone a shift and a postprocessing algorithm 3 which enables the data emanating from the reading of the basic watermark 4 and from the co-watermark 5 to be made reliable. These algorithms can be used either for the processing of stationary images, or for the watermarking of video images.

The function of the basic watermarking algorithm 1 is to perform a modulation of DCT coefficients of the transformed blocks of the image. Before performing this transformation the image is decomposed into adjacent blocks of size NxN, then each of the blocks is transformed into a block of NxN coefficients F(u,v) obtained through the known relation:

$$F(u,v) = 4/N^{2}.c(u).c(v).\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y).\frac{\cos(2x+1).u.pi.}{2N}.\frac{\cos(2y+1).v.pi}{2N}$$

with u=0 to N-1
v=0 to N-1
c(i)=½√2 for i=0
c(i)=1 for i=1 to N-1

As shown by the example of Figure 2 each block 4 of the image of NxN pixels gives rise to a block 5 of NxN DCT coefficients. In a block of the image, each pixel is referenced by its co-ordinates (x,y) with respect to the origin of the block. Likewise, each coefficient of the DCT block is referenced by its co-ordinates (u,v)

with respect to the origin of the block. The embedding of a watermarking message is achieved by modifying in the manner represented in Figures 2 and 3 certain component coefficients of the DCT blocks. The blocks and their coefficients are chosen randomly in the manner represented in Figure 4 by means of a block address generator 6 which determines the coefficients to be modified in each of the blocks. Each bit b_i of the message to be embedded is associated with a block of the image. This bit is embedded by modifying two DCT coefficients c_0 and c_1 of this block.

The choice of these coefficients depends on the key; they are in general chosen within the low frequencies of the image, that is to say those which are to be found in the bottom left corner of the DCT coefficient blocks. For security reasons only two coefficient values c_0 and c_1 are selected as shown in Figure 3 by random drawing. This selection is performed in a manner represented in Figure 4 from a random generator of block addresses 6 which for each bit b_i selects two addresses with coefficient $(u_0\ v_0)$ and $(u_1\ v_1)$. A map of the pairs c_0 and c_1 of selected DCT coefficients is stored in a memory space 7. The watermarking proper is subsequently carried out by modifying the values of the coefficients c_0 and c_1 according to the process described by the processing steps 9 to 19 represented on the flowchart of Figure 5. According to this process the absolute values of the DCT coefficients of each pair of coefficients c_0, c_1 calculated in step 9 are compared in step 10 with a specified threshold value S. If the result of the comparison performed in step 10 is not less than the threshold S the coefficient block is rejected in step 11 and the process goes to step 14 to the analysis of the pair of coefficients of the next block. Conversely if in step 10 the result of the comparison is less than the threshold S the phase of embedding the bit b_1 is executed by modifying the value of the pairs of the selected DCT coefficients. This

modification is carried out by executing steps 12 to 17_b, transforming each pair of coefficients (c_0,c_1) into a new pair (c'_0,c'_1) in a one-to-one manner via a function f, such that the function f complies with the relation $|c'_1|-|c'_0|\geq d$. If in step 12 the value of the bit b_i to be embedded is 0 then the absolute value of the coefficient c_1 takes in step 13_a the absolute value $|c'_1|$ obtained by adding a specified growth value d to the absolute value of the coefficient c'_0. In the converse case if in step 12 the value of the bit b_i to be written is 1, it is the value of the other coefficient c_0 which is modified in step 13_b, taking as absolute value $|c'_0|$ that obtained by adding the growth value d to the absolute value of the coefficient c'_1. Tests are executed in steps 15_a and 15_b to determine the signs of the coefficients c'_0 and c'_1. If the result of a test 15_a, 15_b, is positive the sign given to the coefficient c'_0 respectively c'_1 is positive, on the other hand the sign becomes negative in the converse case as is depicted in steps 16_a, 16_b and 17_a, 17_b.

To offset the fact that certain bits b_i may be unusable because they lead to values of coefficients c_0, c_1 for which the test of step 10 is positive, the algorithm is repeated on all the blocks of the image, this leading for example, for a television picture standard comprising 576 lines and 720 columns per frame, to the use of a message word enabling 6480 blocks to be watermarked.

On reception the reading of the watermarking message which is performed in step 5 of the flowchart of Figure 1 takes place in the manner represented in steps 18 to 22 of the flowchart of Figure 6 by decoding the pairs of coefficients c_0, c_1 corresponding to each of the bits bi of the watermarking message. In step 18 the absolute value of the difference of the absolute values of the pairs of coefficients c_0, c_1 is compared with the threshold value S which was used on transmission when

embedding the bit b_i. If the result of the comparison is positive the value of the corresponding bit b_i is regarded as undetermined in step 19 and the process goes to the decoding of the pair of coefficients c_0 c_1 of the block of coefficients corresponding to the next embedded bit b_{i+1}. On the other hand if in step 18 the result of the test is negative, the value of the bit b_i can be determined and the process goes to the execution of step 20 which consists in comparing with the value zero the difference of the absolute values of the coefficients c_0, c_1 so as to determine in step 21 that the value of the bit b_i is "null" if the result of the comparison of step 20 is positive, or to determine in step 22 that the bit value b_i equals "one" if the result of the comparison of step 20 is negative.

The co-watermarking process depicted in step 2 of the flowchart of Figure 1 makes it possible to retrieve, by executing step 4, the co-ordinates of the origin of the initial image when it is received by a receiver and when it has been chopped or moved in translation, with a view to synchronization for the reading of another watermark for example.

In this case, to retrieve the origin co-ordinates of the image a first solution can consist in using the known "patchwork" algorithm of Messrs William Bender, Daniel Gruhl, and Norishige Morimoto already mentioned. In this case it is sufficient to try all the possible translations, to calculate the sum S of the luminance differences of the pairs of points of the image, retaining as origin co-ordinates only those for which the sum S is a maximum. However, this reading procedure is complicated and takes time.

The co-watermarking method according to the invention makes it possible to simplify this procedure appreciably by effectively remedying the problem encountered in the transmission of stationary images or

moving images which may undergo a shift as a result of the processings introduced by the MPEG, JPEG coders or the recording hardware for example. Without an origin label, the reading of a watermark bearing a message is in fact difficult to see [sic] impossible.

According to the invention the co-watermarking process uses a binary pseudo-random matrix P of size mxm in the image, of zero average and whose autocorrelation function is the smallest possible away from the origin. As shown by Figure 7 this matrix is obtained by symmetrizing an m-sequence of bits. In the example, the equation of the generating polynomial is $x^4 + x^3 + 1$, but other forms of primitive polynomials may also be used. The matrix P is used to build an image I_p of the size of the image to be watermarked I by periodic repetition of the latter in the manner represented in Figure 8. The luminance values I(i,j) of the pixels with co-ordinates (i,j) in the image I are modified by applying to the latter a plus or minus marking amplitude d depending on the binary state "+1" or "-1" of the corresponding pixels of the binary image I_p according to the relations:

$$I'(i,j)=I(i,j)+d \quad \text{if } I_p(i,j)=1 \quad (2)$$

$$I'(i,j)=I(i,j)-d \quad \text{if } I_p(i,j)=-1 \quad (3)$$

In relations (2) and (3) the marking amplitude can be made to depend on the image so as to reduce the visibility of the marking.

On reception the reading of the watermarked image takes place in the manner represented in Figure 9, building from the watermarked image I' received an image matrix M of size mxm according to the relation:

$$M(i,j) = \sum_{k=0}^{k=p} \sum_{l=0}^{l=q} I'(km+i, lm+j) \quad (4)$$

$$\text{with } p < \frac{N-i}{m} \text{ and } q < \frac{N-j}{m}$$

this corresponding to summing the blocks of size NxN of the image.

A cross-correlation calculation between the matrix M and the original binary matrix P is subsequently performed on all the possible shifts of the matrix M. This calculation is performed according to the relation:

$$S(x,y) = \sum_{i=0}^{i} \sum_{j=0}^{j} M(i,j)P((i+x) \bmod m, (j+y) \bmod m) \quad (5)$$

$$\text{with } i < m \text{ and } j < m$$

as a result of the calculation the co-ordinates xo and yo adopted for the origin are those for which the number S(xo,yo) is a maximum.

The co-watermarking algorithm makes it possible to retrieve the co-ordinates of the origin modulo the number m. Naturally when m=N the size of the original image, then the conditions of the "patchwork" algorithm of the prior art hold.

The purpose of executing the postprocessing step 3 of the flowchart of Figure 1 is to examine the reliability of the data emanating from the basic watermarking in particular in automatic checking applications when the conditions of transmission are poor, in the case for example of MPEG transmissions at very low bit rate. The algorithm used uses the redundancy introduced when writing the watermark and with the aid of statistical criteria gives an estimate of the quality and of the reliability of the message read out. This redundancy takes the form of an intra-image redundancy or of a

temporal redundancy. Intra-image redundancy may be utilized in the case of the watermarking of stationary images and video images. It is due to the use of error correcting codes or repetitions when writing the message. The temporal redundancy is achieved by repeating the same message on each video image, it makes it possible to estimate the quality of the message read out by giving a priori an idea of the distribution of the bits of the message read out. By assuming for example that a single bit is embedded while being repeated 10 times in the image, in this case, the message read out if it is error-free, is of the form: 1111111111 or 0000000000. If after transmission the message read is of the form 0001000000, it means that there has been at least one error and it can then be assumed with sufficiently great confidence that the 0 bit has been sent. If on the other hand the message read out is of the form 0111010011 then it is possible to decide that the 1 bit has been sent since 6 bits are in the 1 state and 4 bits are in the 0 state. However, as in the latter case the confidence in this result appears to be lower and it is more judicious not to decide.

An implementation of this algorithm is illustrated in the flowchart of Figure 10. In this flowchart S_{0i} denotes the number of times or [sic] a bit b_i of rank i of the message has been read has [sic] the value 0 and S_{1i} denotes the number of times or [sic] this same bit has been read with the value 1. In step 23 a first test is performed to compare the numbers S_{0i} and S_{1i}. If the number S_{0i} is less than the number S_{1i} then it is decided in step 24 that there have been S_{0i} transmission errors and that the bit sent probably had the value 1, on the other hand if in the converse case the number S_{0i} is greater than the number S_{1i} it is decided in step 25 that there have been S_{1i} transmission errors and that the bit b_i sent probably had the value 0. The degree of confidence to be accorded to these results is

subsequently determined in the next step 27 by a binomial test of them, modelled by the Bernouilli binomial probability law. If the quality of the test appears to be sufficient the bit b_i is allowed in step 27 in the converse case it is disallowed in step 28. On completion of steps 27 and 28 the system goes to the test of the next bit b_{i+1} of the message received.

Claims

1. Process for watermarking images for the processing and transmission of stationary or video images of the type consisting in embedding (1) in the images before their transmission, a message by modifying the data characteristic of the images, characterized in that it consists in performing a co-watermarking (2) by periodic embedding of a binary matrix P into the image so as to determine on reception the co-ordinates of the origin of the initial image and allow the registration of the images received relative to this origin so as to make it possible to read the embedded message.

2. Process according to Claim 1, characterized in that the co-watermarking binary matrix is a pseudo-random matrix P of size mxm obtained by symmetry of a binary m-sequence.

3. Process according to either of Claims 1 and 2, characterized in that it consists in building an image I_p of the size of the watermarked image by periodic repetition of the pseudo-random matrix P, and in modifying the luminance values I(i,j) of pixels with co-ordinates (i,j) of the image which are homologous to those of the image obtained by periodic repetition of the co-watermarking matrix by a marking amplitude depending for each pixel on the value of the homologous pixel in the image obtained by periodic repetition of the watermarking matrix.

4. Process according to Claim 2, characterized in that, to determine at reception the co-ordinates of the origin of the initial image, it consists in chopping the image received into blocks, in summing the blocks to form a matrix M of size mxm, in cross-correlating the matrix M with the co-watermarking binary matrix P by successive shifts of the matrix M relative to the matrix P, and in taking as co-ordinates of the origin

the co-ordinates for which the cross-correlation product is a maximum.

5. Process according to any one of Claims 1 to 4, characterized in that, to perform a watermarking (1) on video images, it consists in transforming the image into blocks of DCT coefficients, in embedding a message into the image by modulating the DCT coefficients (9,..22) so as to perform an adaptive marking in order to achieve invisibility of the embedded message upon the restoration of the image, and in rendering the message robust to degradations by the use of a redundancy.

6. Process according to Claim 5, characterized in that it consists in associating with each bit b_i of the message to be embedded two coefficients of a block of DCT coefficients and in modifying (10,...17) the values of the two coefficients selected as a function of the binary value of the bit of the message to be embedded.

7. Process according to Claim 6, characterized in that, to perform the watermarking, it consists in comparing (10) the difference of the absolute values of the pairs of coefficients chosen from each block with a specified threshold value S so as to modify (13,...17) the absolute value of one of them as a function of the binary state of the bit of the message to be embedded when the result of the comparison is less than the specified threshold value S.

8. Process according to any one of Claims 5 to 7, characterized in that, to read the watermark of a video image, it consists in decoding the pairs of DCT coefficients corresponding to the bits of the embedded message by comparing (18) the absolute value of the difference of the absolute values of the pairs of coefficients with the specified threshold value S, in comparing (20) with the zero value the difference of

the absolute values of the pairs of coefficients so as to determine the binary state of the corresponding embedded bits when the result of the comparison is less than the value of the threshold S or in declaring (19) the binary state of the embedded bits as being undetermined if the result of the comparison is greater than the value of the threshold S.

9. Process according to any one of Claims 1 to 8, characterized in that it consists in performing a watermarking on all the points of the image.

10. Process according to any one of Claims 1 to 9, characterized in that it consists in performing a postprocessing (3; 23,…,28) on the images received so as to estimate the quality and the reliability of the embedded message by using the redundancy of the embedded message.

11. Process according to Claim 10, characterized in that it consists in repeating the watermarking message on each video image during a specified number of times by comparing (2, 3) for each bit of the watermarking message the number of times it is received according to a first state and the number of times it is received according to a second state, and in comparing (26) the totalized values thus obtained with a specified threshold value determined by the Bernouilli binomial probability law.

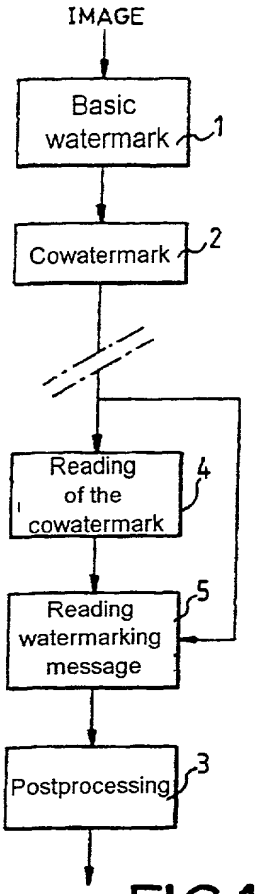

FIG.1

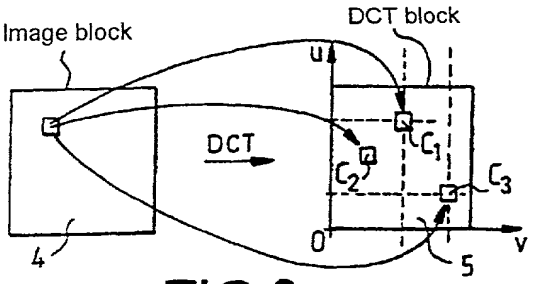

FIG.2

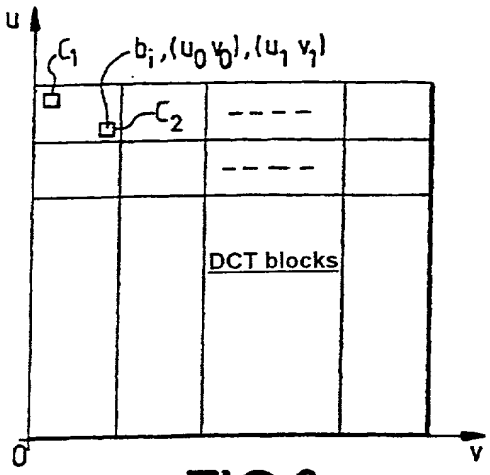

FIG.3

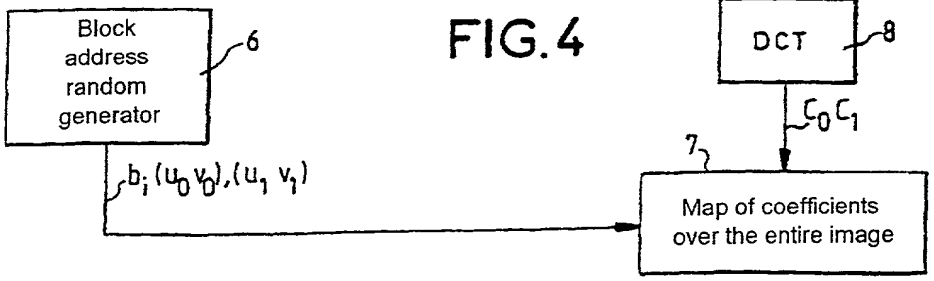

FIG.4

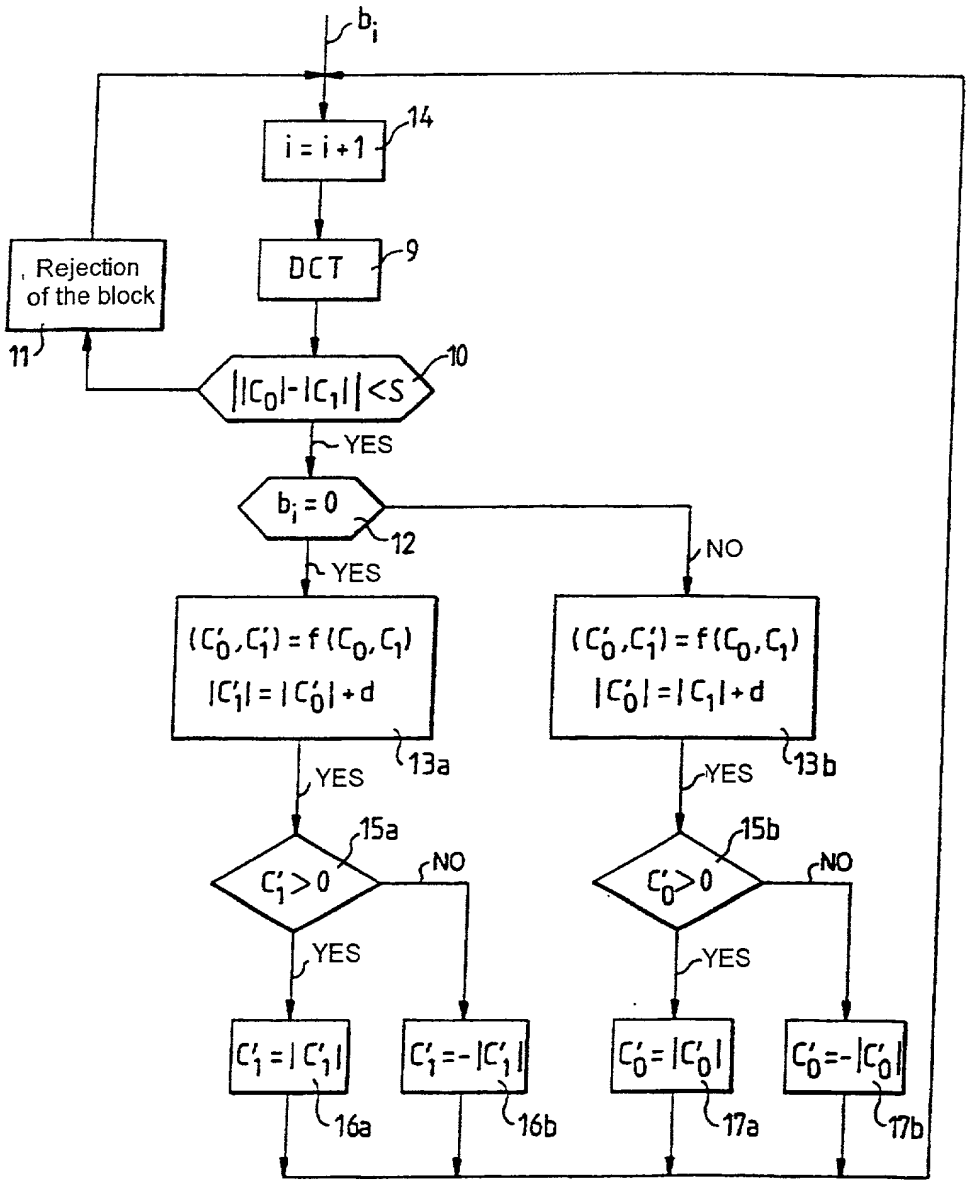
b_i
i = i + 1
14
DCT
9
Rejection of the block
11
$||C_0|-|C_1||<S$
10
YES
$b_i = 0$
12
NO
YES
$(C'_0, C'_1) = f(C_0, C_1)$
$|C'_1| = |C'_0| + d$
13a
$(C'_0, C'_1) = f(C_0, C_1)$
$|C'_0| = |C_1| + d$
13b
YES
YES
15a
$C'_1 > 0$
NO
15b
$C'_0 > 0$
NO
YES
YES
$C'_1 = |C'_1|$
16a
$C'_1 = -|C'_1|$
16b
$C'_0 = |C'_0|$
17a
$C'_0 = -|C'_0|$
17b

FIG. 5

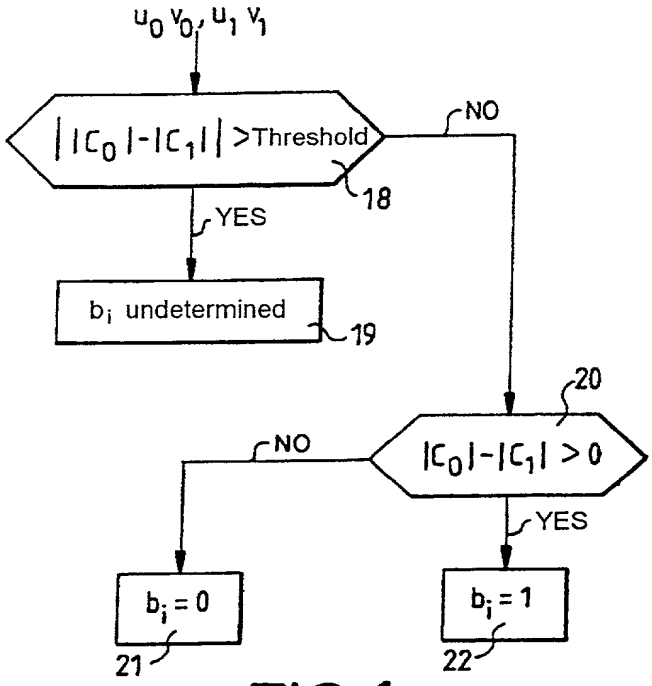
u_0 v_0, u_1 v_1
$|C_0|-|C_1|$ >Threshold
NO
18
YES
b_i undetermined
19
20
NO
$|C_0|-|C_1|$ > 0
YES
b_i = 0
21
b_i = 1
22

FIG.6

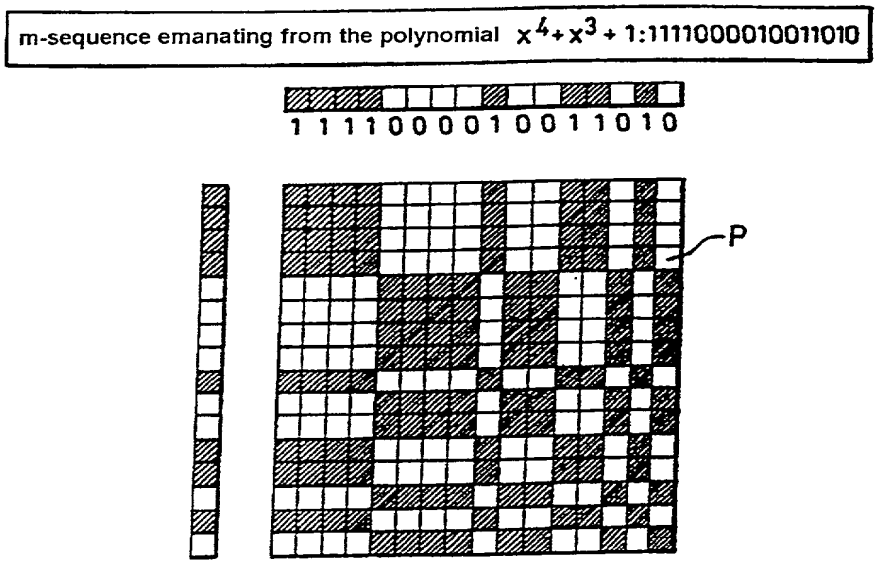
m-sequence emanating from the polynomial x^4+x^3+1:1111000010011010
1 1 1 1 0 0 0 0 1 0 0 1 1 0 1 0
P

FIG.7

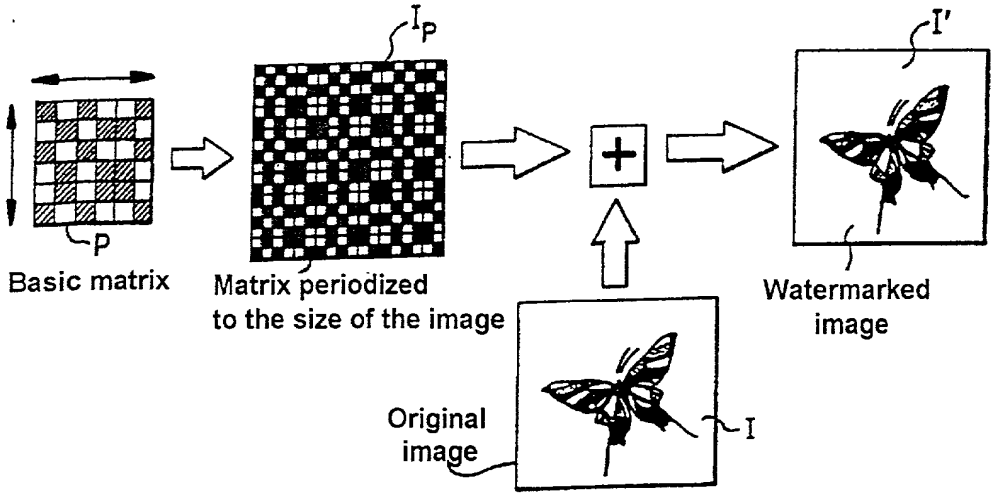
I_P
I'
P
Basic matrix
Matrix periodized
to the size of the image
Watermarked
image
Original
image
I

FIG. 8

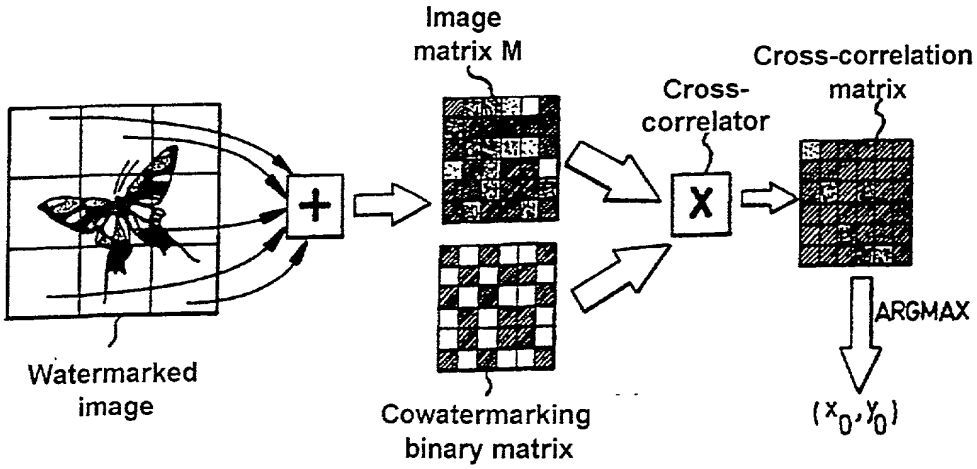
Image
matrix M
Cross-correlation
matrix
Cross-
correlator
X
ARGMAX
(x_0, y_0)
Watermarked
image
Cowatermarking
binary matrix

FIG. 9

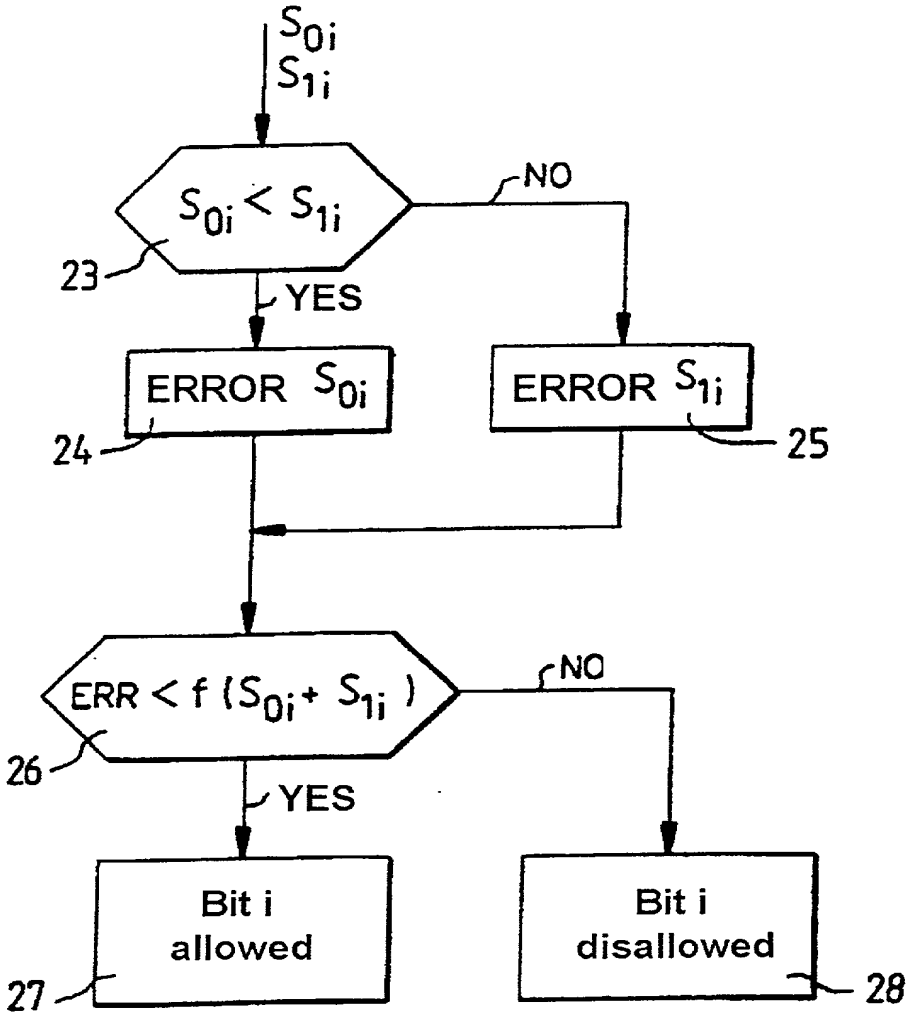
S_{0i}
S_{1i}
$S_{0i} < S_{1i}$
NO
23
YES
ERROR S_{0i}
ERROR S_{1i}
24
25
ERR < f (S_{0i} + S_{1i})
NO
26
YES
Bit i allowed
Bit i disallowed
27
28

FIG. 10

Declaration and Power of Attorney for Patent Application
Déclaration et Pouvoirs pour Demande de Brevet

French Language Declaration

En tant l'inventeur nommé ci-après, je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon domicile, mon adresse postale et ma nationalité sont ceux figurant ci-dessous à côté de mon nom.

My residence, post office address and citizenship are as stated next to my name.

Je crois être le premier inventeur original et unique (si un seul nom est mentionné ci-dessous), ou l'un des premiers co-inventeurs originaux (si plusieurs noms sont mentionnés ci-dessous) de l'objet revendiqué, pour lequel une demande de brevet a été déposée concernant l'invention intitulée

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

PROCESS FOR WATERMARKING IMAGES

et dont la description est fournie ci-joint à moins

- ☐ ci-joint
- ☐ a été déposée le _____

  sous le numéro de demande des Etats-Unis ou le numéro de demande international PCT

  _____ et modifiée le

  _____ (le cas échéant).

the specification of which:

- ☐ is attached hereto.
- ☒ was filed on April 7, 2000

  as United States Application Number or PCT International Application Number

  PCT/FR00/00900 and was amended on

  _____ (if applicable).

Je déclare par le présent acte avoir passé en revue et compris le contenu de la description ci-dessus, revendications comprises, telles que modifiées par toute modification dont il aura été fait référence ci-dessus.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

French Language Declaration

Je revendique par le présent acte avoir la priorité étrangère, en vertu du Titre 35, § 119(a)-(d) ou § 365(b) du Code des Etats-Unis, sur toute demande étrangère de brevet ou certificat d'inventeur ou, en vertu du Titre 35, § 365(a) du même Code, sur toute demande internationale PCT désignant au moins un pays autre que les Etats-Unis et figurant ci-dessous et, en cochant la case, j'ai aussi indiqué ci-dessous toute demande étrangère de brevet, tout certificat d'inventeur ou toute demande internationale PCT ayant une date de dépôt précédant celle de la demande à propos de laquelle une priorité est revendiquée

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)
Demande(s) de brevet antérieure(s) dans un autre pays

(Number) (Numéro)	(Country) (Pays)	(Day/Month/Year Filed) (Jour/Mois/Anné de dépôt)	Priority claimed Droit de priorité revendiqué: Yes Oui	No Non
99 05194 ✓	FRANCE ✓	23 APRIL 1999 ✓	XX ☐	☐
			☐	☐

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 119(e) du Code des Etats-Unis, de toute demande de brevet provisoire effectuée aux Etats-Unis et figurant ci-dessous

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below

(Application No.) (Nº de demande)	(Filing Date) (Date de dépôt)	(Application No.) (Nº de demande)	(Filing Date) (Date de dépôt)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 120 du Code des Etats-Unis, de toute demande de brevet effectuée aux Etats-Unis, ou en vertu du Titre 35, § 365(c) du même Code, de toute demande internationale PCT désignant les Etats-Unis et figurant ci-dessous et, dans la mesure où l'objet de chacune des revendications de cette demande de brevet n'est pas divulgué dans la demande antérieure américaine ou internationale PCT, en vertu des dispositions du premier paragraphe du Titre 35, § 112 du Code des Etats-Unis, je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations, dont j'ai pu disposer entre la date de dépôt de la demande antérieure et la date de dépôt de la demande nationale ou internationale PCT de la présente demande.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application No.) (Nº de demande)	(Filing Date) (Date de dépôt)	(Status) (patented, pending, abandoned) (Statut) (breveté, en cours d'examen, abandonné)
PCT/FR00/00900 ✓	7 APRIL 2000 ✓	

Je déclare par le présent acte que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d' une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des Etats-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIRS. En tant que l'inventeur cité, je désigne par la présente l'(les) avocat(s) et/ou agent(s) suivant(s) pour qu'ils poursuive(nt) la procédure de cette demande de brevet et traite(nt) toute affaire s'y rapportant avec l'Office des brevets et des marquees: *(mentionner le nom et le numéro d'enregistrement)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: *(list name and registration number)*

Norman F. Oblon, Reg. No. 24,618; Marvin J Spivak, Reg. No. 24,913, C. Irvin McClelland, Reg No. 21,124; Gregory J. Maier, Reg No.25,599; Arthur I. Neustadt, Reg. No. 24,854; Richard D. Kelly, Reg. No. 27,757; James D. Hamilton, Reg. No. 28,421; Eckhard H. Kuesters, Reg. No. 28,870; Robert T. Pous, Reg. No. 29,099; Charles L. Gholz, Reg. No. 26,395, Vincent J. Sunderdick, Reg. No 29,004; William E. Beaumont, Reg No. 30,996; Steven B Kelber, Reg. No. 30,073; Robert F. Gnuse, Reg No. 27,295; Jean-Paul Lavalleye, Reg. No. 31,451; Stephen G. Baxter, Reg. No. 32,884; Martin M. Zoltick, Reg. No. 35,745; Robert W. Hahl, Reg. No. 33,893; Richard L. Treanor, Reg No. 36,379; Steven P. Weihrouch, Reg. No. 32,829; John T Goolkasian, Reg. No. 26,142; Marc R. Labgold, Reg. No. 34,651; William J. Healey, Reg. No. 36,160; Richard L. Chinn, Reg. No. 34,305, Steven E. Lipman, Reg. No. 30,011; Carl E. Schlier, Reg. No. 34,426; James J. Kulbaski, Reg. No. 34,648; Catherine B. Richardson, Reg. No 39,007; Richard A. Neifeld, Reg No. 35,299; and J. Derek Mason, Reg. No. 35,270, with full powers of substitution and revocation.

30-

Addresser toute correspondance à:

Send Correspondence to:
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
FOURTH FLOOR
1755 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VIRGINIA 22202 U.S.A.

Adresser tout appel téléphonique à:
(nom et numéro de téléphone)

Direct Telephone calls to: *(name and telephone number)*
(703) 413-3000

Nom complete de l'unique ou premier inventeur	Full name of sole or first inventor Séverine BAUDRY
1-00 Date	September 17, 2001 Date
Signature de l'inventeur	Inventor's signature Séverine Baudry
Domicile	Residence 95250 BEAUCHAMP FRX FRANCE
Nationalité	Citizenship French
Adresse Postale	Post Office Address 44, avenue du Général Leclerc
	95250 BEAUCHAMP FRANCE
Nom complete du second co-inventeur, le cas echeant	Full name of second joint inventor, if any Didier NICHOLSON
2-00 Date	September 17, 2001 Date
Signature de l'inventeur	Second inventor's signature Didier NICHOLSON
Domicile	Residence 92600 ASNIERES S/SEINE FRX FRANCE
Nationalité	Citizenship French
Adresse Postale	Post Office Address 20, rue Bapst
	92600 ASNIERES S/SEINE FRANCE

(Fournier les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)

French Language Declaration

Nom complet du troisième co-inventeur, le cas echeant	Full name of third joint inventor, if any
3-00	Catherine SIMON September 17, 2001
Signature de l'inventeur Date	Third Inventor's signature Date
Domicile	Residence 92210 SAINT-CLOUD ~~FRX~~ FRANCE
Nationalité	Citizenship French
Adresse Postale	Post Office Address 124, boulevard de la République
	92210 SAINT-CLOUD FRANCE

Nom complet du quatrième co-inventeur, le cas echeant	Full name of fourth joint inventor, if any
4-00	Philippe N'GUYEN September 17, 2001
Signature de l'inventeur Date	Fourth Inventor's signature Date
Domicile	Residence 92100 BOULOGNE BILLANCOURT FRANCE
Nationalité	Citizenship French FRX.
Adresse Postale	Post Office Address 101, avenue J.B. Clément
	92100 BOULOGNE BILLANCOURT FRANCE

Nom complet du cinquième co-inventeur, le cas echeant	Full name of fifth joint inventor, if any
Signature de l'inventeur Date	Fifth Inventor's signature Date
Domicile	Residence
Nationalité	Citizenship
Adresse Postale	Post Office Address

Nom complet du sixième co-inventeur, le cas echeant	Full name of sixth joint inventor, if any
Signature de l'inventeur Date	Sixth Inventor's signature Date
Domicile	Residence
Nationalité	Citizenship
Adresse Postale	Post Office Address

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)